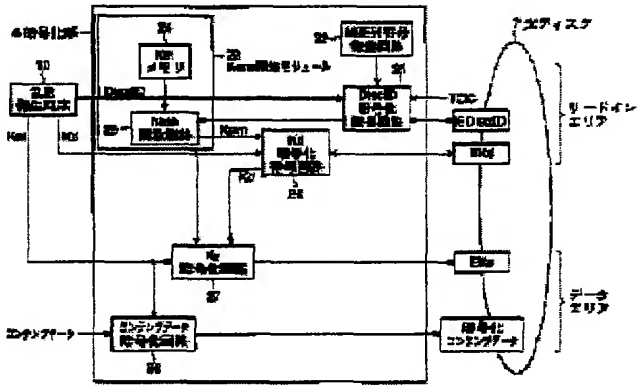
INFORMATION PROCESSOR, INFORMATION METHOD, PROVIDING MEDIUM AND RECORDING MEDIUM

Publication number: JP11224461
Publication date: 1999-08-17
Inventor: ASANO TOMOYUKI; OSAWA YOSHITOMO; HASHIMOTO MEGUMI
Applicant: SONY CORP
Classification:
- international: ***G11B20/10; G06F21/24; G09C1/00; H04L9/32;*** **G11B20/10; G06F21/00; G09C1/00; H04L9/32;** (IPC1-7): G11B20/10; G09C1/00; H04L9/32
- European:
Application number: JP19980025310 19980206
Priority number(s): JP19980025310 19980206

Abstract of **JP11224461**

PROBLEM TO BE SOLVED: To obtain intrincic information in a recording medium by decoding the intrincic information in the recording medium which are read out from the medium and are ciphered with an M series code. SOLUTION: At first, a disk ID encryption decoding circuit 21 receives an EDiscID which is read out from the read-in area of an optical disk 7 and which is an ciphered DiscID. Next, the circuit 21 generates an EDiscID by decoding the EDiscID based on the predetermined M series code which is suppied from an M series code generating circuit 22 to output it to the hash function circuit 25 of an effective master key generating module 23. Moreover, M series codes to be supplied from the circuit 22 are codes which are given when proper licences are granted from copyright holders.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平11－224461

(43)公開日　平成11年(1999)８月17日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ
Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ　1/00	６６０Ｄ
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ｅ

審査請求　未請求　請求項の数９　ＯＬ　（全 11 頁）

(21)出願番号　特願平10－25310

(22)出願日　平成10年(1998)２月６日

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号

(72)発明者　浅野　智之
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(72)発明者　大澤　義知
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(72)発明者　橋本　恵
東京都品川区北品川６丁目７番35号　ソニー株式会社内

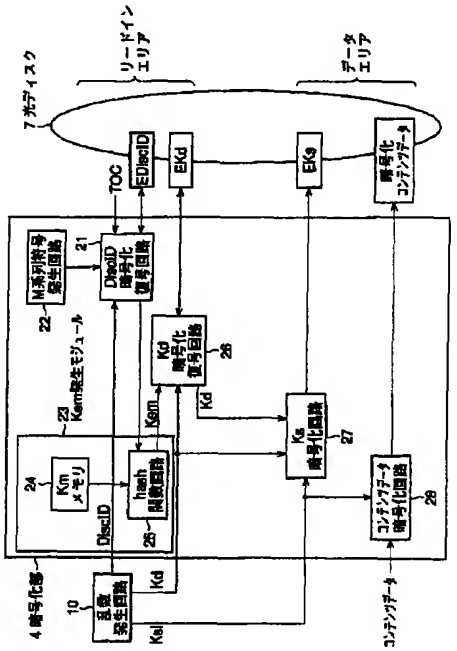
(74)代理人　弁理士　稲本　義雄

(54)【発明の名称】　情報処理装置、情報処理方法、提供媒体、および記録媒体

(57)【要約】

【課題】　記録媒体から読み出された暗号化された記録媒体の固有情報をM系列符号で復号し、記録媒体の固有情報を得る。

【解決手段】　ステップＳ３１において、DiscID暗号化復号回路２１は、光ディスク７のリードインエリアから読み出された、暗号化されたDiscIDであるEDiscIDを受け取る。DiscID暗号化復号回路２１はさらに、ステップＳ３２において、M系列符号発生回路２２から供給された予め定められたM系列符号に基づいて、EDiscIDを復号して、DiscIDを生成し、Kcm発生モジュール２３のhash関数回路２５に出力する。M系列符号回路２２が供給するM系列符号は、著作権者から適正なライセンスを受けるときに、与えられたものである。



1

【特許請求の範囲】

【請求項１】　着脱可能な記録媒体に情報を記録または再生する情報処理装置において、

第１の秘密キーを発生する発生手段と、

前記記録媒体からそこに記録されている暗号化された前記記録媒体の固有情報を受信する受信手段と、

前記発生手段により発生された第１の秘密キーにより、前記受信手段により受信した暗号化された前記記録媒体の固有情報を復号し、前記記録媒体の固有情報を生成する生成手段とを備えることを特徴とする情報処理装置。

【請求項２】　前記記録媒体から暗号化された前記記録媒体の固有情報を受信できないとき、乱数を発生する乱数発生手段と、

前記第１の秘密キーにより、前記乱数を前記記録媒体の固有情報として暗号化し、前記記録媒体に記録する記録手段とをさらに備えることを特徴とする請求項１に記載の情報処理装置。

【請求項３】　前記生成手段により生成された前記記録媒体の固有情報と、第２の秘密キーに基づいて、第３の秘密キーを算出する算出手段と、

前記算出手段により算出された前記第３の秘密キーに対応して、所定の情報を暗号化し、前記記録媒体に記録する記録手段とをさらに備えることを特徴とする請求項１に記載の情報処理装置。

【請求項４】　前記所定の情報は、前記記録媒体に固有の秘密キーであることを特徴とする請求項３に記載の情報処理装置。

【請求項５】　前記第３の秘密キーにより、前記記録媒体から再生された前記記録媒体に固有の暗号化されている第４の秘密キーを復号する復号手段をさらに備え、

前記記録手段に、復号された前記第４の秘密キーを利用して、所定の情報を暗号化し、前記記録媒体に記録することを特徴とする請求項３に記載の情報処理装置。

【請求項６】　前記第３の秘密キーにより、前記記録媒体から再生された前記記録媒体に固有の暗号化されている第４の秘密キーを復号する第１の復号手段と、

復号された前記第４の秘密キーを利用して、前記記録媒体から供給された暗号化されているデータを復号する第２の復号手段とをさらに備えることを特徴とする請求項３に記載に情報処理装置。

【請求項７】　着脱可能な記録媒体に情報を記録または再生する情報処理装置の情報処理方法において、

第１の秘密キーを発生する発生ステップと、

前記記録媒体からそこに記録されている暗号化された前記記録媒体の固有情報を受信する受信ステップと、

前記発生ステップにより発生された第１の秘密キーにより、前記受信ステップにより受信した暗号化された前記記録媒体の固有情報を復号し、前記記録媒体の固有情報を生成する生成ステップとを備えることを特徴とする情報処理方法。

2

【請求項８】　着脱可能な記録媒体に情報を記録または再生する情報処理装置に使用するコンピュータプログラムであって、

第１の秘密キーを発生する発生ステップと、

前記記録媒体からそこに記録されている暗号化された前記記録媒体の固有情報を受信する受信ステップと、

前記発生ステップにより発生された第１の秘密キーにより、前記受信ステップにより受信した暗号化された前記記録媒体の固有情報を復号し、前記記録媒体の固有情報を生成する生成ステップとを備えるコンピュータプログラムを提供することを特徴とする提供媒体。

【請求項９】　情報処理装置に装着され、情報が記録または再生される記録媒体において、

M系列符号で暗号化した前記記録媒体に固有の情報が記録されていることを特徴とする記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、情報処理装置、情報処理方法、提供媒体、および記録媒体に関し、特に、より安全にデータを授受することを可能にする情報処理装置、情報処理方法、提供媒体、および記録媒体に関する。

【０００２】

【従来の技術】近年、情報をデジタル的に記録する記録機器および記録媒体が普及しつつある。これらの記録機器および記録媒体は、例えば、映像や音楽のデータを劣化させることなく記録し、再生するので、データを、その質を維持しながら何度もコピーすることができる。しかしながら、映像や音楽のデータの著作権者にしてみれば、自らが著作権を有するデータが、その質を維持しながら何度も不正にコピーされ、市場に流通してしまう恐れがある。このため、記録機器および記録媒体の側で、著作権を有するデータが不正にコピーされるのを防ぐ必要がある。

【０００３】例えば、ミニディスク（MD）（商標）システムにおいては、SCMS(Serial CopyManagement System)と呼ばれる方法が用いられている。これは、デジタルインタフェースによって、音楽データとともに伝送される情報のことである。この情報は、音楽データが、copy free、copy once allowed、またはcopy prohibitedのうちのいずれのデータであるのかを表す。ミニディスクレコーダは、デジタルインタフェースから音楽データを受信した場合、SCMSを検出し、これが、copy prohibitedであれば、音楽データをミニディスクに記録せず、copy once allowedであれば、これをcopy prohibitedに変更し、受信した音楽データとともに記録し、copy freeであれば、これをそのまま、受信した音楽データとともに記録する。

【０００４】このようにして、ミニディスクシステムにおいては、SCMSを用いて、著作権を有するデータが不正

にコピーされるのを防いでいる。

【０００５】また、著作権を有するデータが不正にコピーされるのを防ぐ別の例としては、Digital Versatile Disk(DVD)（商標）システムにおける、コンテンツスクランブルシステムがあげられる。このシステムでは、ディスク上の、著作権を有するデータが全て暗号化され、ライセンスを受けた記録機器だけが暗号鍵を与えられ、これにより暗号化されたデータを復号し、意味のあるデータを得ることができるようになされている。そして、記録機器は、ライセンスを受ける際に、不正コピーを行わない等の動作規定に従うように設計される。このようにして、DVDシステムにおいては、著作権を有するデータが不正にコピーされるのを防いでいる。

【０００６】

【発明が解決しようとする課題】しかしながら、上記のミニディスクシステムが採用している方式では、SCMSがcopy once allowedであれば、これをcopy prohibitedに変更し、受信したデータとともに記録するなどの動作規定に従わない記録機器が、不正に製造されてしまう。

【０００７】また、上記のDVDシステムが採用している方式は、ROMメディアに対しては有効であるが、ユーザがデータを記録可能なRAMメディアにおいては有効ではない。RAMメディアにおいては、不正者は、暗号を解読できない場合であっても、ディスク上のデータを全部、新しいディスクに不正にコピーすることによって、ライセンスを受けた正当な記録機器で動作するディスクを新たに作ることができるからである。

【０００８】本発明はこのような状況に鑑みてなされたものであり、例えば、著作権者から適正に利用許可を受けた者にだけ与えられる秘密キーに基づいて、記録媒体に固有の情報にアクセスできるようにすることで、不正コピーを防止するものである。

【０００９】

【課題を解決するための手段】請求項１に記載の情報処理装置は、第１の秘密キーを発生する発生手段と、記録媒体からそこに記録されている暗号化された記録媒体の固有情報を受信する受信手段と、発生手段により発生された第１の秘密キーにより、受信手段により受信した暗号化された記録媒体の固有情報を復号し、記録媒体の固有情報を生成する生成手段とを備えることを特徴とする。

【００１０】請求項７に記載の情報処理方法は、第１の秘密キーを発生する発生ステップと、記録媒体からそこに記録されている暗号化された記録媒体の固有情報を受信する受信ステップと、発生ステップにより発生された第１の秘密キーにより、受信ステップにより受信した暗号化された記録媒体の固有情報を復号し、記録媒体の固有情報を生成する生成ステップとを備えることを特徴とする情報処理方法。

【００１１】請求項８に記載の提供媒体は、第１の秘密キーを発生する発生ステップと、記録媒体からそこに記録されている暗号化された記録媒体の固有情報を受信する受信ステップと、発生ステップにより発生された第１の秘密キーにより、受信ステップにより受信した暗号化された記録媒体の固有情報を復号し、記録媒体の固有情報を生成する生成ステップとを備えるコンピュータプログラムを提供することを特徴とする。

【００１２】請求項９に記載の記録媒体は、M系列符号で暗号化した記録媒体に固有の情報が記録されていることを特徴とする。

【００１３】請求項１に記載の情報処理装置、請求項７に記載の情報処理方法、および請求項８に記載の提供媒体においては、第１の秘密キーが発生され、記録媒体からそこに記録されている暗号化された記録媒体の固有情報が受信され、発生された第１の秘密キーにより、受信した暗号化された記録媒体の固有情報が復号され、記録媒体の固有情報が生成される。

【００１４】

【発明の実施の形態】以下に本発明の実施の形態を説明するが、特許請求の範囲に記載の発明の各手段と以下の実施の形態との対応関係を明らかにするために、各手段の後の括弧内に、対応する実施の形態（但し一例）を付加して本発明の特徴を記述すると、次のようになる。但し勿論この記載は、各手段を記載したものに限定することを意味するものではない。

【００１５】請求項１に記載の情報処理装置は、第１の秘密キー（予め定められたM系列符号）を発生する発生手段（例えば、図３のM系列符号発生回路２２）と、記録媒体からそこに記録されている暗号化された記録媒体の固有情報（EDiscID）を受信する受信手段（例えば、図３のDiscID暗号化復号回路２１）と、発生手段により発生された第１の秘密キーにより、受信手段により受信した暗号化された記録媒体の固有情報を復号し、記録媒体の固有情報（DiscID）を生成する生成手段（例えば、図３のDiscID暗号化復号回路２１）とを備えることを特徴とする。

【００１６】請求項２に記載の情報処理装置は、記録媒体から暗号化された記録媒体の固有情報を受信できないとき、乱数を発生する乱数発生手段（例えば、図３の乱数発生回路１０）と、第１の秘密キーにより、乱数を記録媒体の固有情報として暗号化し、記録媒体に記録する記録手段（例えば、図３のDiscID暗号化復号回路２１）とをさらに備えることを特徴とする。

【００１７】請求項３に記載の情報処理装置は、生成手段により生成された記録媒体の固有情報と、第２の秘密キー（マスタキーKm)に基づいて、第３の秘密キー（イフェクティブマスタキーKem）を算出する算出手段（例えば、図３のhash関数回路２５）と、算出手段により算出された第３の秘密キーに対応して、所定の情報を暗号化し、記録媒体に記録する記録手段（例えば、図３のKd

暗号化復号回路２６）とをさらに備えることを特徴とする。

【００１８】請求項５に記載の情報処理装置は、第３の秘密キーにより、記録媒体から再生された記録媒体に固有の暗号化されている第４の秘密キー（暗号化ディスクキーEKd）を復号する復号手段（例えば、図３のKd暗号化復号回路２６）をさらに備え、記録手段に、復号された第４の秘密キー（マスタキーKd）を利用して、所定の情報を暗号化し、記録媒体に記録することを特徴とする。

【００１９】請求項６に記載の情報処理装置は、第３の秘密キーにより、記録媒体から再生された記録媒体に固有の暗号化されている第４の秘密キーを復号する第１の復号手段（例えば、図４のEKd復号回路５６）と、復号された第４の秘密キーを利用して、記録媒体から供給された暗号化されているデータを復号する第２の復号手段（例えば、図４のEKs暗号化回路５７およびコンテンツデータ復号回路５８）とをさらに備えることを特徴とする。

【００２０】図１は、本発明を適用した光ディスク記録再生装置の構成例を表している。入力部１は、ボタン、スイッチ、リモートコントローラなどにより構成され、ユーザにより入力操作されたとき、その入力操作に対応する信号を出力する。制御回路２は、記憶されている所定のコンピュータプログラムに従って、装置全体を制御する。

【００２１】記録再生回路３は、暗号化部４と復号部５を有し、復号部５は、ピックアップ６により、光ディスク７から再生されたデータを復号し、外部に再生信号として出力する。暗号化部４は、外部から記録信号の供給を受け取ると、これを暗号化し、ピックアップ６に供給して、光ディスク７に記録させる。

【００２２】ピックアップ６は、レーザビームを光ディスク７に照射することで、データの記録再生を行う。スピンドルモータ９は、サーボ回路８によって制御され、光ディスク７を回転させる。

【００２３】サーボ回路８は、スピンドルモータ９を駆動することにより、光ディスク７を所定の速度で（例えば線速度一定で）回転させる。サーボ回路８はまた、ピックアップ６のトラッキングおよびフォーカシングの他、スレッドサーボを制御する。乱数発生回路１０は、制御回路２の制御により、所定の乱数を発生する。

【００２４】光ディスク７には、図２に示すような構造を有するデータが記録されている。光ディスク７のリードインエリアには、光ディスクのID（以下、DiscIDと称する）を予め定められたM系列符号で暗号化したEDiscID、デイスクキーKdをイフェクティブマスタキーKemで暗号化した暗号化ディスクキーEKdが記録されている。

【００２５】M系列符号は、所定の周期で、”０”と”１”の２値がランダムに出現する疑似ランダム２値信号（一種の疑似乱数）であり、DiscIDは、例えば、ファイル名やデイレクトリ情報などのTOC(Table Of Contents)データ内に、予め設定された所定のM系列符号に基づいて埋め込むことで暗号化されている。すなわち、DiscIDは、TOCデータのエッジの時間ずれとして記録される。このような暗号化を行うと、TOCデータはM系列符号がなくとも読み取ることができるが（TOCデータは暗号化されないが）、DiscIDはM系列符号がないと読み取る（復号する）ことができなくなる。このようなM系列符号に基づく暗号化に関する技術は、特願平09-288960号として本出願人が先に提案している。なお、この所定のM系列符号は、著作権者から適正なライセンスを受ける際、後述するマスタキーKmとともに、ライセンスを受けた者に与えられる。

【００２６】イフェクティブマスタキーKemは、式（１）に従い、マスタキーKmとDiscIDの結合にhash関数を適用して計算される。

$$\text{イフェクティブマスタキーKem} = \text{hash}(\text{マスタキーKm} + \text{DiscID}) \qquad (1)$$

ここでマスタキーKmは、著作権者等から適正にライセンスを受けた者（光ディスク記録再生装置）にだけ与えられる秘密のキーである。また、ここで、例えば、ＡとＢの結合とは、それぞれが３２ビットであるとき、Ａの後方にＢを結合して、６４ビットのデータとすることを意味する。

【００２７】光ディスク７のデータエリアの各セクタSi(i=1,2,...)は、ヘッダおよびメインデータ部で構成され、ヘッダには、セクタキーKsiをディスクキーKdで暗号化した暗号化セクタキーEKsi(i=1,2,...)が格納されている（ここでKsiのiは、セクタの番号を示し、セクタキーはセクタ毎に異なるのでKsiと記述するが、特に区別する必要がない場合は、Ksとも記述する）。メインデータ部には、コンテンツデータをセクタキーKsiで暗号化した暗号化コンテンツデータが格納されている。

【００２８】図３は、暗号化部４の構成例を表している。DiscID暗号化復号回路２１は、光ディスク７から読み出されたEDiscIDを、M系列符号発生回路２２から供給されるM系列符号に基づいて復号し、DiscIDを生成する。DiscID暗号化復号回路２１はまた、乱数発生回路１０から発生された乱数をDiscIDとして受け取り、M系列符号発生回路２２から供給されるM系列符号に基づいて、上述したように、入力されるTOC情報に埋め込むように暗号化して、EDiscIDを生成し、光ディスク７に記録する。

【００２９】M系列符号発生回路２２は、例えば、直列接続された複数のフリップフロップとイクスクルーシブオア回路からなり、所定のM系列符号を発生するようになされている。あるいは、ROM、EEPROMなどで構成することもできる。

【００３０】Kem発生モジュール２３のKmメモリ２４は、マスタキーKmを記憶する。Kem発生モジュール２３のhash関数回路２５は、マスタキーKmとDiscIDの結合を生成し、これにhash関数を適用してイフェクティブマスタキーKemを算出する。

【００３１】Kd暗号化復号回路２６は、光ディスク７から読み出された暗号化ディスクキーEKdを、イフェクティブマスタキーKemで復号して、ディスクキーKdを生成する。Kd暗号化復号回路２６はまた、乱数発生回路１０から発生された乱数をディスクキーKdとして受け取り、イフェクティブマスタキーKemで暗号化して暗号化ディスクキーEKdを生成し、光ディスク７に記録する。

【００３２】Ks暗号化回路２７は、乱数発生回路１０から発生された乱数をセクタキーKsとして受け取り、ディスクキーKdで暗号化して暗号化セクタキーEKsを生成し、光ディスク７に記録する。コンテンツデータ暗号化回路２８は、セクタキーKsで、コンテンツデータを暗号化し、光ディスク７に記録する。

【００３３】次に、図４に、復号部５の構成例を示す。EDiscID復号回路５１は、光デイスク７から読み出されたEDiscIDを、M系列符号発生回路５２から供給されるM系列符号に基づいて復号して、DiscIDを生成する。M系列符号発生回路５２は、M系列符号回路２２と同様の構成を有し、M系列符号発生回路２２と同一のM系列符号を発生するようになされている。

【００３４】Kem発生モジュール５３のKmメモリ５４は、マスタキーKmを記憶する。Kem発生モジュール５３のhash関数回路５５は、マスタキーKmとDiscIDの結合を生成し、これにhash関数を適用してイフェクティブマスタキーKemを計算する。このKem発生モジュール５３は、Kem発生モジュール２３と同一の構成とされ、両者を兼用するようにしてもよい。

【００３５】EKd復号回路５６は、光ディスク７から読み出された暗号化ディスクキーEKdを、イフェクティブマスタキーKemで復号して、ディスクキーKdを算出する。EKs復号回路５７は、光ディスク７から各セクタSiのヘッダに記録されている暗号化セクタキーEKsを読み出し、ディスクキーKdで復号して、セクタキーKsを算出する。コンテンツデータ復号回路５８は、光ディスク７から読み出された暗号化されたコンテンツデータを、セクタキーKsで復号する。

【００３６】次に、ユーザデータが光デイスク７に記録される場合の暗号化部４における処理手順を、図５のフローチャートを参照して説明する。なお、この例の場合、DiscIDは、光ディスク７製造時に、光ディスク７に書き込まれているものとする。

【００３７】最初に、ステップＳ３１において、DiscID暗号化復号回路２１は、光ディスク７のリードインエリアから読み出された、暗号化されているDiscIDであるEDiscIDを受け取る。DiscID暗号化復号回路２１はさらに、ステップＳ３２において、M系列符号発生回路２２から供給された所定のM系列符号に基づいて、EDiscIDを復号して、DiscIDを生成し、Kem発生モジュール２３のhash関数回路２５に出力する。M系列符号回路２２が供給するM系列符号は、著作権者から適正なライセンスを受けるときに、与えられたものである。

【００３８】ステップＳ３３において、Kem発生モジュール２３のhash関数回路２５は、Kem発生モジュール２３のKmメモリ２４から、マスタキーKmを読み出す。Kem発生モジュール２３のhash関数回路２５はさらに、ステップＳ３４で、上述の式（１）に従い、光ディスク７のDiscIDとマスタキーKmの結合にhash関数を適用して、イフェクティブマスタキーKemを計算し、Kd暗号化復号回路２６に供給する。

【００３９】次に、ステップＳ３５において、Kd暗号化復号回路２６は、光ディスク７のリードインエリアから読み出された暗号化ディスクキーEKdを受け取る。Kd暗号化復号回路２６は、ステップＳ３６で、光ディスク７のリードインエリアに、暗号化ディスクキーEKdが書き込まれているか否か（暗号化ディスクキーEKdを受け取ることができたか否か）の判定を行う。暗号化ディスクキーEKdが書き込まれていないと判定された場合、ステップＳ３７に進み、乱数発生回路１０は、４０ビットの乱数を発生し、ディスクキーKdとして、Kd暗号化復号回路２６に出力する。

【００４０】次に、ステップＳ３８において、Kd暗号化復号回路２６は、乱数発生回路１０から供給されたディスクキーKdを、hash関数回路２５から受け取ったイフェクティブマスタキーKemにより暗号化して、暗号化ディスクキーEKdを生成し、光ディスク７のリードインエリアに記録する。

【００４１】ステップＳ３６で、暗号化ディスクキーEKdが書き込まれていると判定された場合、ステップＳ３９に進み、Kd暗号化復号回路２６は、この光ディスク７から読み出された暗号化ディスクキーEKdを、hash関数回路２５から受け取ったイフェクティブマスタキーKemで復号して、ディスクキーKdを得る。Kd暗号化復号回路２６は、そのディスクキーKdを、Ks暗号化回路２７に出力する。

【００４２】ステップＳ３８またはＳ３９の処理の後、乱数発生回路１０は、ステップＳ４０で、４０ビットの乱数を発生し、セクタキーKsとして、Ks暗号化回路２７、およびコンテンツデータ暗号化回路２８に出力する。Ks暗号化回路２７は、ステップＳ４１で、Kd暗号化復号回路２６（暗号化ディスクキーEKdが光ディスク７に記録されている場合）、または乱数発生回路１０（暗号化ディスクキーEKdが光ディスク７に記録されていない場合）から受け取ったディスクキーKdで、乱数発生回路１０から受け取ったセクタキーKsを暗号化して、暗号化セクタキーEKsを生成する。Ks暗号化回路２７はま

た、その暗号化セクタキーEKsを、光ディスク７のデータエリアにあるセクタヘッダに記録する。

【００４３】次に、ステップＳ４２において、コンテンツデータ暗号化回路２８は、（ステップＳ４０で乱数発生回路１０から受け取った）セクタキーKsにより、コンテンツデータを暗号化し、光ディスク７のデータエリアのメインデータ部に記録する。

【００４４】ステップＳ４３において、暗号化部４の各回路は、全てのコンテンツデータを記録したか否かの判定を行う。全てのコンテンツデータがまだ記録されていないと判定された場合、ステップ４４に進み、暗号化部４の各回路は、光ディスク７の、まだデータを記録していないセクタにアクセスし、ステップＳ４０に戻り、以下同様の処理を繰り返す。ステップＳ４３で、全てのコンテンツデータが記録されたと判定された場合、暗号化部４の各回路は、全ての記録処理を終了する。

【００４５】以上のようにして、著作権者から適正なライセンスを受けるときに、与えられた所定のM系列符で、暗号化されたDiscIDを復号し、DiscIDを得ることにより、暗号化した情報が記録媒体に記録される。

【００４６】次に、製造時に、DiscIDが記録されていない光ディスク７に対して、ユーザデータを記録する場合の暗号化部４における処理手順を、図６のフローチャートを参照して説明する。

【００４７】最初に、ステップＳ５１において、DiscID暗号化復号回路２１は、光ディスク７のリードインエリアから読み出されたEDiscIDを受け取り、またKd暗号化復号回路２６は、光ディスク７のリードインエリアから読み出された暗号化ディスクキーEKdを受け取る。

【００４８】次に、ステップＳ５２において、DiscID暗号化復号回路２１は、光ディスク７のリードインエリアに、EDiscIDが書き込まれているか否か（EDiscIDを受けることができたか否か）の判定を行い、Kd暗号化復号回路２６は、光ディスク７のリードインエリアに、暗号化ディスクキーEKdが書き込まれているか否か（暗号化ディスクキーEKdを受け取ることができたか否か）の判定を行う。EDiscIDと暗号化ディスクキーEKdが共に書き込まれていないと判定された場合、ステップＳ５３に進み、乱数発生回路１０は、１２８ビットの乱数を発生し、DiscIDとして、DiscID暗号化復号回路２１に出力する。

【００４９】次に、ステップＳ５４において、DiscID暗号化復号回路２１は、乱数発生回路１０から供給されたDiscIDを、M系列符号発生回路２２から供給されたM系列符号に基づいて、上述したように、TOC情報中に埋め込むようにして暗号化して、EDiscIDを生成し、光ディスク７のリードインエリアに記録する。

【００５０】次に、ステップＳ５５において、Kem発生モジュール２３のhash関数回路２５は、Kem発生モジュール２３のKmメモリ２４から、マスタキーKmを読み出す。Kem発生モジュール２３のhash関数回路２５は、ステップＳ５６で、上述の式（１）に従い、光ディスク７のDiscID、およびKmメモリ２４から読み出したマスタキーKmの結合にhash関数を適用して、イフェクティブマスタキーKemを計算し、Kd暗号化復号回路２６に供給する。

【００５１】次に、ステップＳ５７において、乱数発生回路１０は、４０ビットの乱数を発生し、ディスクキーKdとして、Kd暗号化復号回路２６に出力する。Kd暗号化復号回路２６は、ステップＳ５８において、乱数発生回路１０から供給されたディスクキーKdを、hash関数回路２５から受け取ったイフェクティブマスタキーKemにより暗号化して、暗号化ディスクキーEKdを生成し、光ディスク７のリードインエリアに記録する。

【００５２】ステップＳ５２で、EDiscIDと暗号化ディスクキーEKdが書き込まれていると判定された場合、ステップＳ５９に進み、DiscID暗号化復号回路２１は、この光ディスクから読み出されたEDiscIDを、M系列符号回路２２から供給されたM系列符号で復号して、DiscIDを生成する。

【００５３】ステップＳ６０において、Kem発生モジュール２３のhash関数回路２５は、Kem発生モジュール２３のKmメモリ２４から、マスタキーKmを読み出す。Kem発生モジュール２３のhash関数回路２５は、ステップＳ６１で、上述の式（１）に従い、光ディスク７のDiscIDとマスタキーKmの結合にhash関数を適用して、イフェクティブマスタキーKemを計算し、Kd暗号化復号回路２６に供給する。

【００５４】次に、ステップＳ６２において、Kd暗号化復号回路２６は、この光ディスク７から読み出された暗号化ディスクキーEKdを、hash関数回路２５から受け取ったイフェクティブマスタキーKemで復号して、ディスクキーKdを得る。Kd暗号化復号回路２６は、ディスクキーKdを、Ks暗号化回路２７に出力する。

【００５５】ステップＳ５８またはＳ６２の処理の後は、ステップＳ６３に進むが、ステップＳ６３乃至Ｓ６７で行われる処理は、図５のステップＳ４０乃至Ｓ４４で行われる処理と同様の処理であり、全てのコンテンツデータが記録されたと判定された場合、全ての記録処理が終了する。

【００５６】以上のようにして、DiscIDが生成され、記録媒体に記録され、そして生成されたDiscIDとマスタキーKmに対応して暗号化されたコンテンツデータが記録媒体に記録される。このことより、例えば、既存の記録媒体（DiscIDが記録されていない記録媒体）に複製されたコンテンツデータを、著作権者から適正にライセンスを受けていない者は、意味のある情報として再生することができない。

【００５７】次に、図７のフローチャートを参照して、復号部５により行われる、ユーザデータの再生処理を説

明する。最初に、ステップＳ８１において、EDiscID復号回路５１は、光ディスク７のリードインエリアから読み出された、暗号化されたDiscIDであるEDiscIDを受け取る。EDiscID復号回路５１はさらに、ステップＳ８２において、M系列符号発生回路５２から供給されたM系列符号に基づいて、EDiscIDを復号してDiscIDを生成し、Kem発生モジュール５３のhash関数回路５５に出力する。

【００５８】次に、ステップＳ８３において、Kem発生モジュール５３のhash関数回路５５は、EDiscID復号回路５１から出力されたDiscIDを受け取るとともに、Kmメモリ５４からマスタキーKmを読み出し、上述の式（１）に従い、光ディスク７のDiscIDとマスタキーKmの結合にhash関数を適用してイフェクティブマスタキーKemを算出し、EKd復号回路５６に供給する。

【００５９】ステップＳ８４において、EKd復号回路５６は、光ディスク７のリードインエリアから読み出された暗号化ディスクキーEKdを受け取る。EKd復号回路５６は、ステップＳ８５で、この読み出された暗号化ディスクキーEKdを、hash関数回路５５から受け取ったイフェクティブマスタキーKemで復号して、ディスクキーKdを算出し、EKs復号回路５７に出力する。

【００６０】次に、ステップＳ８６において、EKs復号回路５７は、光ディスク７のデータエリアから読み出された各セクタの暗号化セクタキーEKsi（i=1,2,...）を受け取る。EKs復号回路５７は、ステップＳ８７で、この読み出された暗号化セクタキーEKsiを、EKd復号回路５６から受け取ったディスクキーKdで復号して、セクタキーKsiを算出し、コンテンツデータ復号回路５８に出力する。

【００６１】ステップＳ８８において、コンテンツデータ復号回路５８は、光ディスク７から読み出された暗号化されているコンテンツデータを受け取る。コンテンツデータ復号回路５８は、ステップＳ８９で、この読み出された暗号化されているコンテンツデータを、EKs復号回路５７から受け取ったセクタキーKsiで復号し、再生信号として出力する。

【００６２】次に、ステップＳ９０において、復号部５の各回路は、光ディスク７のデータエリアから、全てのコンテンツデータを読み出したか否かの判定を行う。全てのコンテンツデータがまだ読み出されていないと判定された場合、ステップＳ９１に進み、復号部５の各回路は、光ディスク７の、まだ読み出されていない次のセクタのデータの供給を受け、ステップＳ８６以降の処理を繰り返す。全てのコンテンツデータが読み出されたと判定された場合、復号部５の各回路は、全ての再生処理を終了する。

【００６３】このように、記録媒体のIDを生成し、所定のM系列符号で暗号化して、記録媒体に記録することで、著作権者から適正にライセンスを受けた者だけが、その記録媒体にアクセスできるようにする。

【００６４】本発明は、光ディスク以外の記録媒体にデータを記録または再生する場合にも適用が可能である。

【００６５】なお、本明細書中において、上記処理を実行するコンピュータプログムをユーザに提供する提供媒体には、磁気ディスク、CD-ROMなどの情報記録媒体の他、インターネット、デジタル衛星などのネットワークによる伝送媒体も含まれる。

【００６６】

【発明の効果】請求項１に記載の情報処理装置、請求項７に記載の情報処理方法、および請求項８に記載の提供媒体によれば、第１の秘密キーにより、記録媒体に記録されている暗号化された記録媒体の固有情報を復号し、記録媒体の固有情報を生成するようにしたので、例えば、予め定められたM系列符号を有していない者が、記録媒体にアクセスすることを困難にする。

【００６７】請求項２に記載の情報処理装置によれば、記録媒体から暗号化された記録媒体の固有情報を受信できないとき、乱数を記録媒体の固有情報として暗号化し、記録媒体に記録するようにしたので、例えば、予め定められたM系列符号を有していない者は、記録媒体の固有情報が記録されていない記録媒体に記録されている情報を、再生することができない。

【００６８】請求項３に記載の情報処理装置によれば、生成手段により生成された記録媒体の固有情報と、第２の秘密キーに基づいて、第３の秘密キーを算出し、算出された第３の秘密キーに対応して、所定の情報を暗号化し、記録媒体に記録するようにしたので、予め定められたM系列符号を有していない者が、記録媒体にアクセスすることを、さらに困難にする。

【００６９】請求項９に記載の記録媒体によれば、M系列符号で暗号化した記録媒体に固有の情報を記録するようにしたので、情報処理装置に記録媒体の固有情報を提供することができる。

【図面の簡単な説明】

【図１】本発明を適用した光ディスク記録再生装置の一実施の形態の構成を示すブロック図である。

【図２】光ディスクに記録されるデータを説明する図である。

【図３】図１の暗号化部４の内部の構成を示す図である。

【図４】図１の復号部５の内部の構成を示す図である。

【図５】図１の暗号化部４の動作を説明するフローチャートである。

【図６】図１の暗号化部４の他の動作を説明するフローチャートである。

【図７】図１の復号部５の動作を説明するフローチャートである。

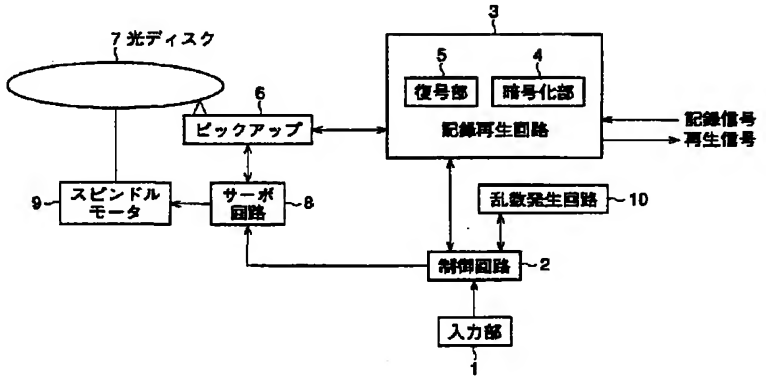
【符号の説明】

１　入力部，２　制御回路，３　記録再生回路，４　暗

13　　14

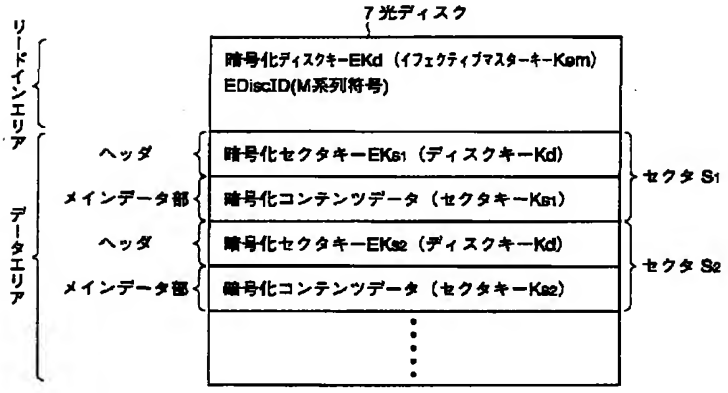
号化部，５　復号部，６　ピックアップ，７　光ディスク，８　サーボ回路，９　スピンドルモータ，１０　乱数発生回路，２１　DiscID暗号化復号回路，２２　M系列符号発生回路，２３　Kem発生モジュール，２４　Km メモリ，２５　hash関数回路，２６　Kd暗号化復号回＊路，２７　Ks暗号化回路，２８　コンテンツデータ暗号化回路，５１　EDiscID復号回路，５２　M系列符号発生回路，５３　Kem発生モジュール，５４　Kmメモリ，５５　hash関数回路，５６　EKd復号回路，５７　EKs復号回路，５８　コンテンツデータ復号回路

【図１】

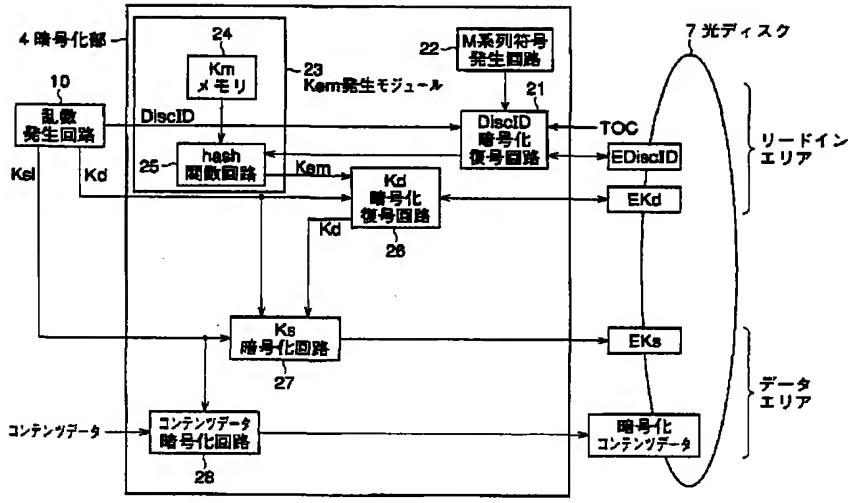


光ディスク記録再生装置

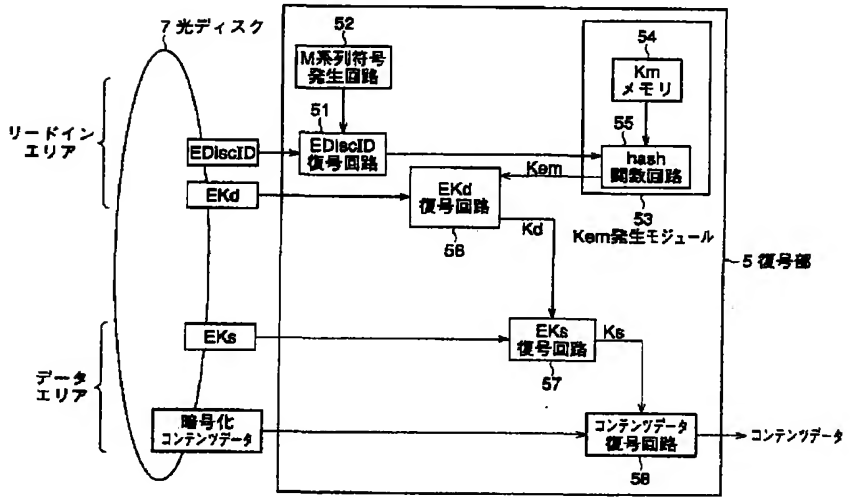
【図２】



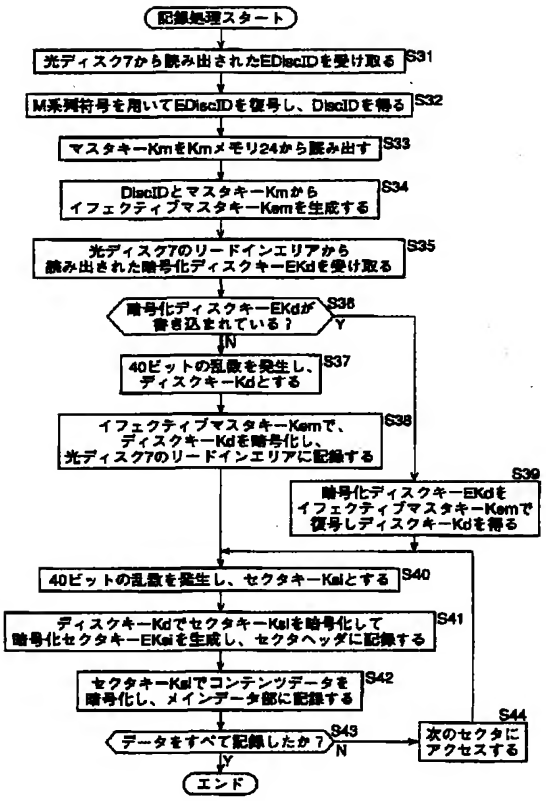
【図３】


4 暗号化部
24
Km
メモリ
23
Kem発生モジュール
22
M系列符号
発生回路
7 光ディスク
10
乱数
発生回路
DiscID
21
DiscID
暗号化
復号回路
TOC
EDiscID
リードイン
エリア
Ksl
Kd
25
hash
関数回路
Kem
Kd
暗号化
復号回路
EKd
Kd
26
Ks
暗号化回路
EKs
27
データ
エリア
コンテンツデータ
コンテンツデータ
暗号化回路
暗号化
コンテンツデータ
28

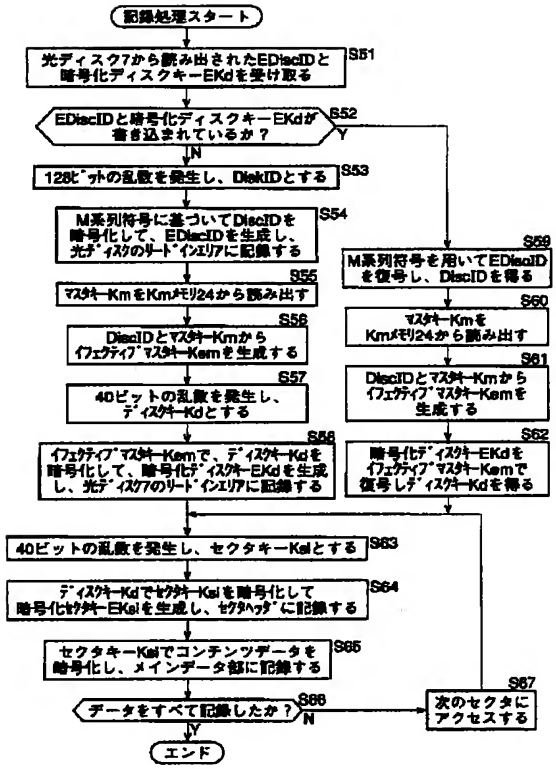
【図４】


7 光ディスク
52
M系列符号
発生回路
54
Km
メモリ
51
55
リードイン
エリア
EDiscID
EDiscID
復号回路
hash
関数回路
EKd
Kem
EKd
復号回路
53
Kem発生モジュール
Kd
5 復号部
58
EKs
EKs
復号回路
Ks
データ
エリア
57
暗号化
コンテンツデータ
コンテンツデータ
復号回路
コンテンツデータ
58

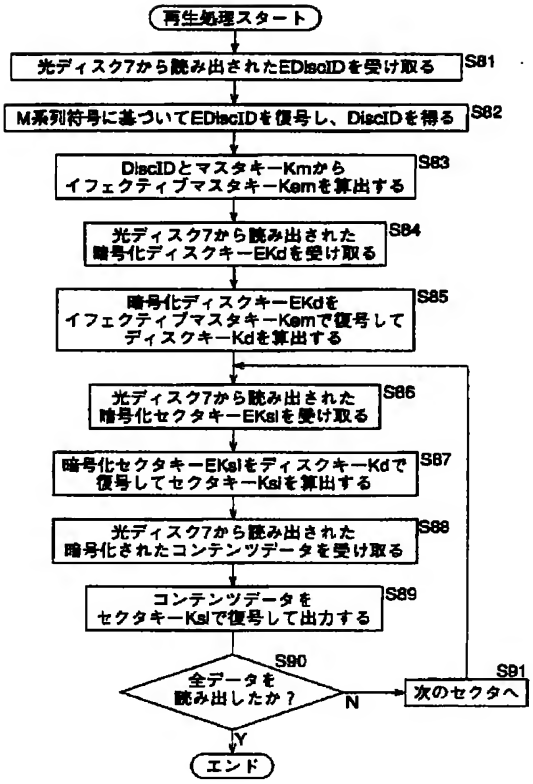
【図５】


記録処理スタート
光ディスク7から読み出されたEDiscIDを受け取る
S31
M系列符号を用いてEDiscIDを復号し、DiscIDを得る
S32
マスタキーKmをKmメモリ24から読み出す
S33
DiscIDとマスタキーKmから
イフェクティブマスタキーKemを生成する
S34
光ディスク7のリードインエリアから
読み出された暗号化ディスクキーEKdを受け取る
S35
暗号化ディスクキーEKdが
書き込まれている？
S36
Y
N
40ビットの乱数を発生し、
ディスクキーKdとする
S37
イフェクティブマスタキーKemで、
ディスクキーKdを暗号化し、
光ディスク7のリードインエリアに記録する
S38
暗号化ディスクキーEKdを
イフェクティブマスタキーKemで
復号しディスクキーKdを得る
S39
40ビットの乱数を発生し、セクタキーKsiとする
S40
ディスクキーKdでセクタキーKsiを暗号化して
暗号化セクタキーEKsiを生成し、セクタヘッダに記録する
S41
セクタキーKsiでコンテンツデータを
暗号化し、メインデータ部に記録する
S42
データをすべて記録したか？
S43
N
Y
次のセクタに
アクセスする
S44
エンド

【図６】


記録処理スタート
光ディスク7から読み出されたEDiscIDと
暗号化ディスクキーEKdを受け取る
S51
EDiscIDと暗号化ディスクキーEKdが
書き込まれているか？
S52
Y
N
128ビットの乱数を発生し、DiskIDとする
S53
M系列符号に基づいてDiscIDを
暗号化して、EDiscIDを生成し、
光ディスクのリードインエリアに記録する
S54
マスタキーKmをKmメモリ24から読み出す
S55
DiscIDとマスタキーKmから
イフェクティブマスタキーKemを生成する
S56
40ビットの乱数を発生し、
ディスクキーKdとする
S57
イフェクティブマスタキーKemで、ディスクキーKdを
暗号化して、暗号化ディスクキーEKdを生成
し、光ディスク7のリードインエリアに記録する
S58
M系列符号を用いてEDiscID
を復号し、DiscIDを得る
S59
マスタキーKmを
Kmメモリ24から読み出す
S60
DiscIDとマスタキーKmから
イフェクティブマスタキーKemを
生成する
S61
暗号化ディスクキーEKdを
イフェクティブマスタキーKemで
復号しディスクキーKdを得る
S62
40ビットの乱数を発生し、セクタキーKsiとする
S63
ディスクキーKdでセクタキーKsiを暗号化して
暗号化セクタキーEKsiを生成し、セクタヘッダに記録する
S64
セクタキーKsiでコンテンツデータを
暗号化し、メインデータ部に記録する
S65
データをすべて記録したか？
S66
N
Y
次のセクタに
アクセスする
S67
エンド

【図７】


再生処理スタート
光ディスク7から読み出されたEDiscIDを受け取る
S81
M系列符号に基づいてEDiscIDを復号し、DiscIDを得る
S82
DiscIDとマスタキーKmから
イフェクティブマスタキーKemを算出する
S83
光ディスク7から読み出された
暗号化ディスクキーEKdを受け取る
S84
暗号化ディスクキーEKdを
イフェクティブマスタキーKemで復号して
ディスクキーKdを算出する
S85
光ディスク7から読み出された
暗号化セクタキーEKsiを受け取る
S86
暗号化セクタキーEKsiをディスクキーKdで
復号してセクタキーKsiを算出する
S87
光ディスク7から読み出された
暗号化されたコンテンツデータを受け取る
S88
コンテンツデータを
セクタキーKsiで復号して出力する
S89
全データを
読み出したか？
S90
N
次のセクタへ
S91
Y
エンド